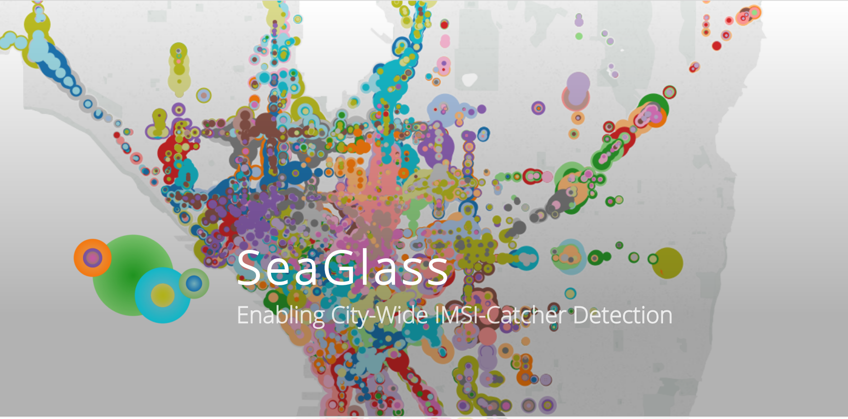


SeaGlass

Enabling City-Wide IMSI-Catcher Detection

City-Wide IMSI-Catcher Detection

SeaGlass is a system designed by security researchers at the University of Washington to measure IMSI-catcher use across a city.

Cellular sensors are built from off-the-shelf parts and installed into volunteers’ vehicles

Sensor data is continuously uploaded from vehicles and aggregated into a city-wide view

Algorithms find anomalies in the cellular network that indicate IMSI-catchers

Bringing Transparency to Cellphone Surveillance

SR II #3
StingRay II
TX ANTENNA
TX1
TX2
TX3
TX4
DF ANTENNA
ANT 1
ANT 2
GPS ANTENNA
RX ANTENNA
RX1
RX2
RX3
CNTRL 1
CNTRL 2
10 MHZ REF OUT
INTERNAL CONTROLLER
10/100
USB
AUX
AUX1
AUX2
PC INPUT
RS232
DC INPUT
12VDC
POWER

Stingray II IMSI-catcher

Source: U.S. Patent and Trademark Office/AP

Modern cellphones are vulnerable to attacks by governments and hackers using rogue cellular transmitters called *IMSI-catchers*. These surveillance devices can precisely locate phones, and sometimes eavesdrop on communications, send spam, or inject malware into phones.

Recent leaks and public records requests have revealed that U.S. law enforcement in Baltimore, Milwaukee, New York, Tacoma, Anaheim, Tucson, and others have used IMSI-catchers extensively in vehicles or aircraft to identify and locate suspects.

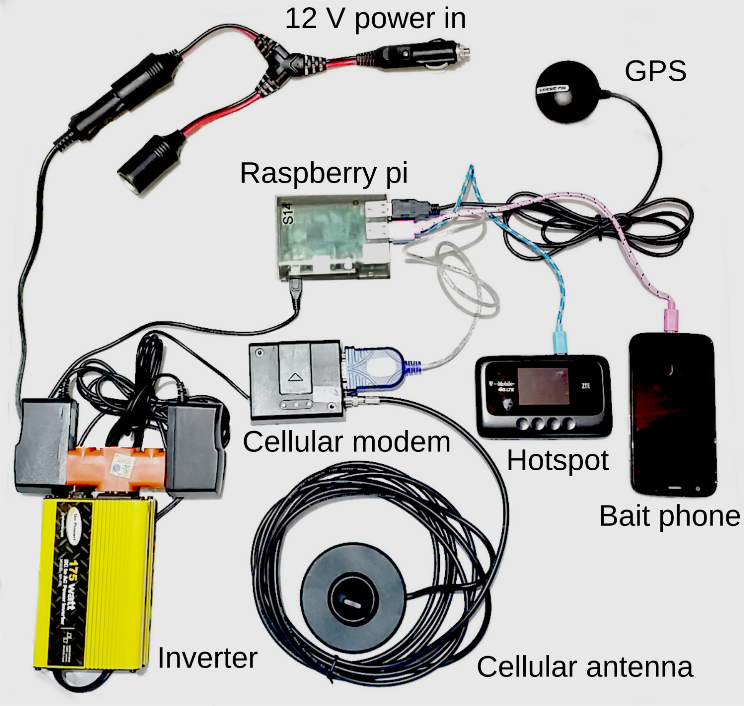
These powerful surveillance devices have often been used with little to no judicial oversight. To provide transparency and accountability, we need independent information on who uses them, how often, and when.

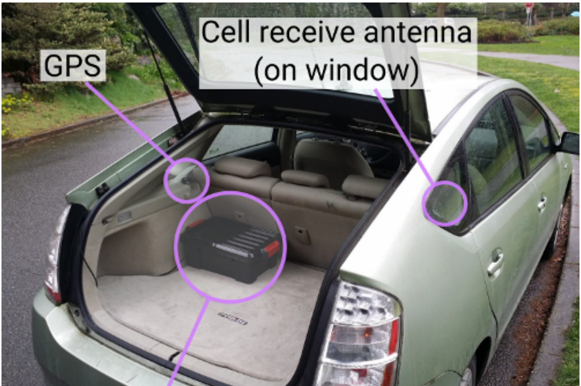
SeaGlass Sensors

SeaGlass sensors collect and upload cell tower signal data to our server where algorithms look for IMSI-catcher signatures.

Main Sensor Parts

- Raspberry Pi computer
- Cellular modem to scan the cell spectrum
- GPS
- Bait cellphone
- Mobile hotspot to upload data





Sensor equipment

SeaGlass sensors are built with off-the-shelf parts, packed into a box, and installed in a vehicle's trunk. Sensors continuously collect and upload cell tower signal data to a cloud server as they drive around the city.

These sensors have advantages over phones because they can contain specialized cellular scanning equipment and external antennas for farther reception ranges. While phone apps can see limited information on the tower currently connected to, our sensors scan the spectrum to measure hundreds of channels at a time and dozens of broadcast properties.

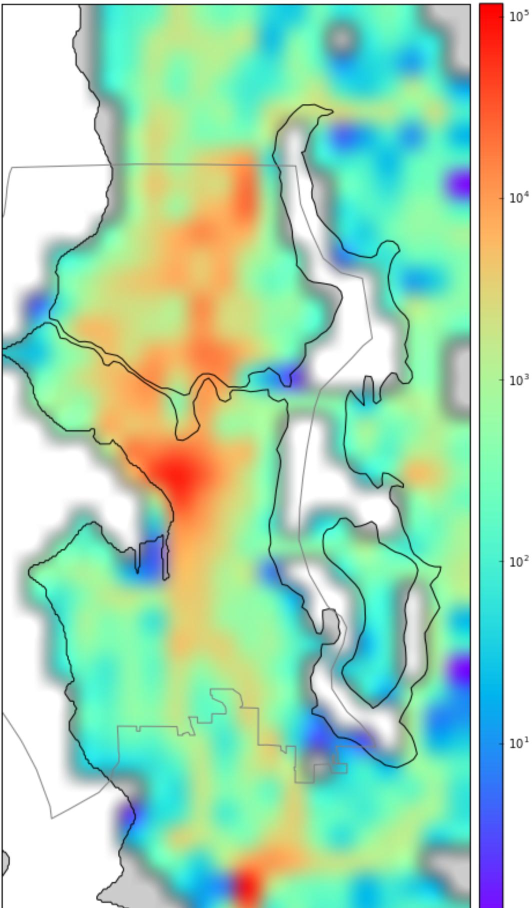
City-Wide Collection

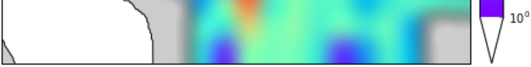
A Two-Month Trial with Ridesharing Volunteers

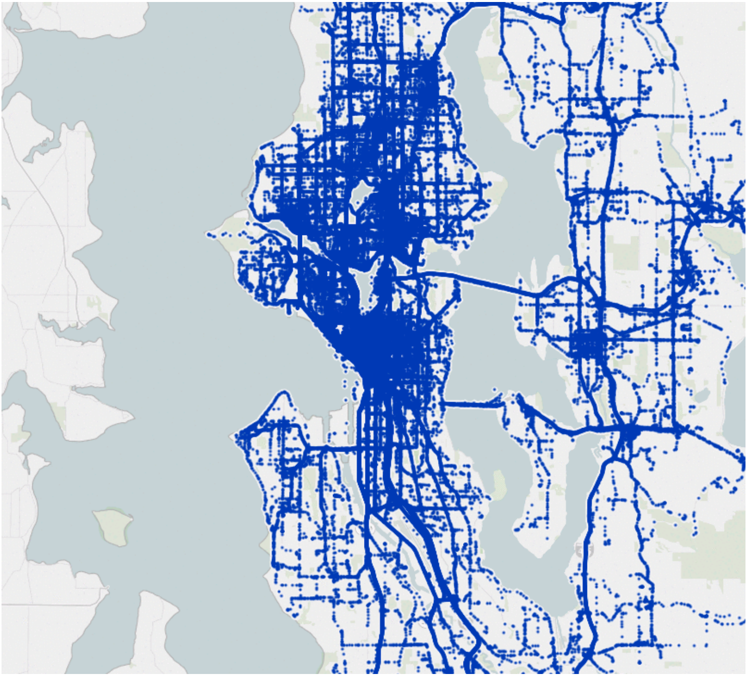
We piloted SeaGlass for two months in Seattle, WA and Milwaukee, WI. Partnering with ridesharing drivers allowed us to collect millions of measurements across both cities.

The measurement coverage in Seattle and Milwaukee is visualized in the following images. Heatmap colors show the number of measurements per square kilometer, and the animated maps show individual locations of cellular scans by SeaGlass sensors over the two-month trial.

Seattle

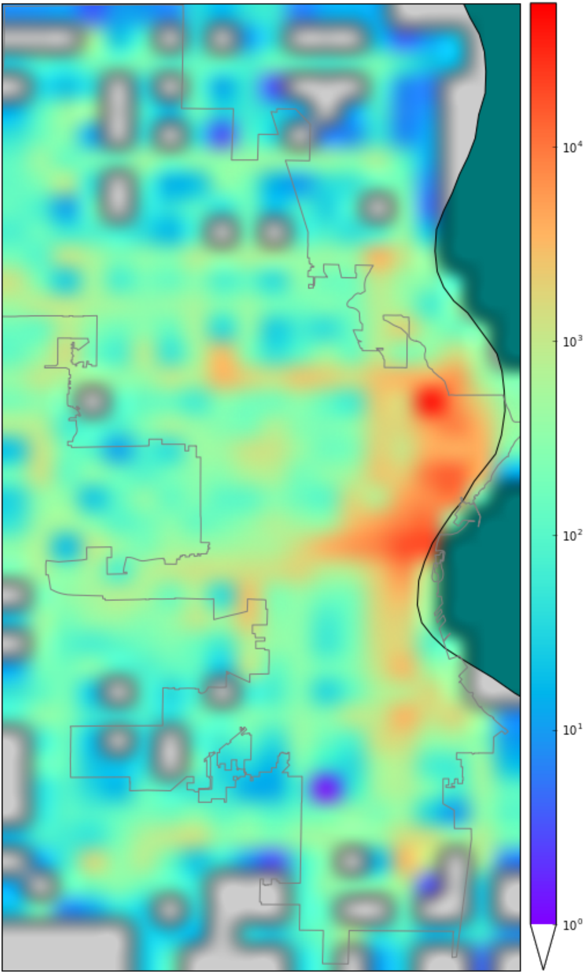


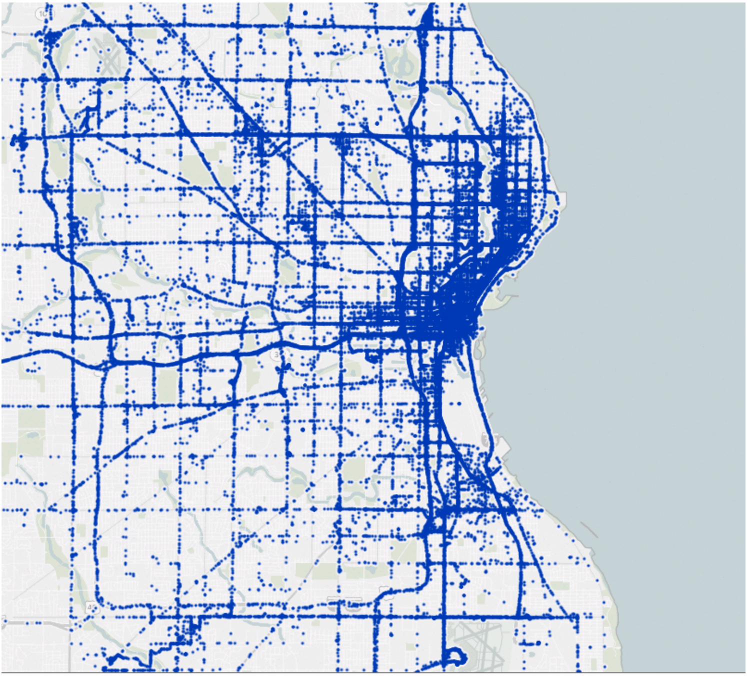




Hover over image to zoom into downtown.

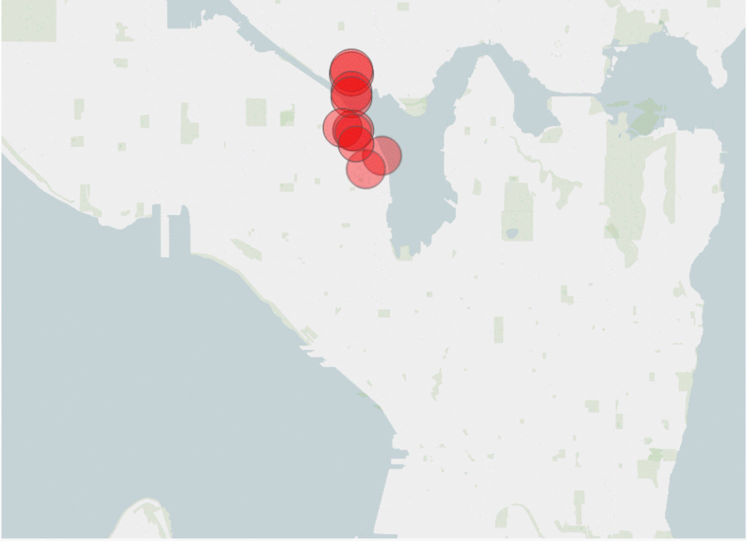
Milwaukee





Hover over image to zoom into downtown.

Aggregating the hundreds or thousands of measurements for each cell tower made from different locations enables us to accurately model the underlying cellular network. We measured more than 1,400 distinct cell tower base stations in Seattle, and over 600 in Milwaukee. As one example, this animation shows a time series of measurements captured from a single cell tower base station around Lake Union in Seattle over two months.



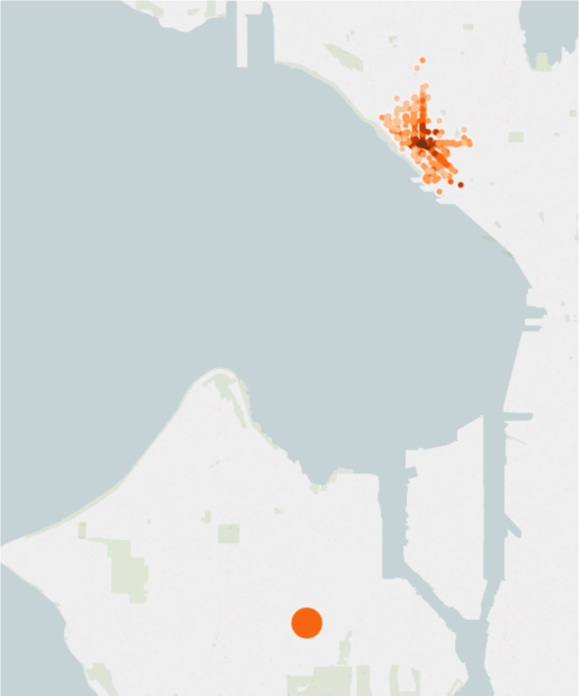
Time series of measurements of one cell tower base station over two months. Higher received signal strengths are red, and lower received signal strengths are in blue.

By modeling the typical behavior of each cell tower over time, SeaGlass can pick out aberrations that indicate the presence of cell-site simulators.

Algorithms

For IMSI-catchers to function as surveillance devices and to operate covertly, they must give off certain *anomaly signatures* that can be detected if you have a sufficiently dense, city-wide view of the cellular network.

We designed detection methods that use the data collected by SeaGlass to automatically flag these anomaly signatures on several features.



Spoofed Transmissions

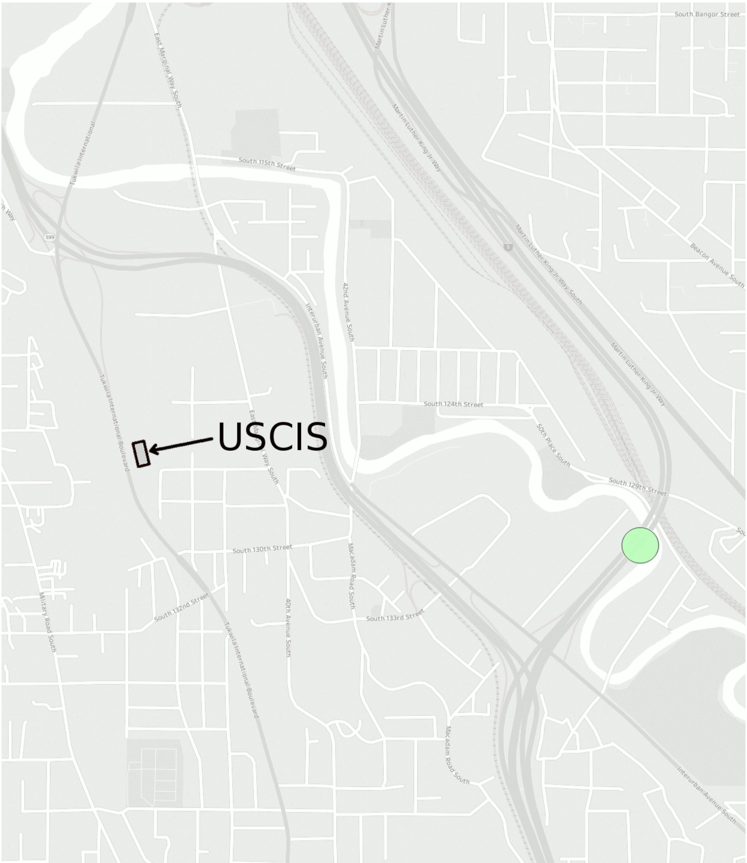
To covertly transmit on the same frequencies as the normal cellular network, IMSI-catchers may mimic the identifying properties (mcc, mnc, cell id, etc.) of legitimate cell towers. We expect IMSI-catchers to prefer transmitting strong signals to capture phones and to be some distance away from the towers they may mimic to avoid interference with the real cell tower.

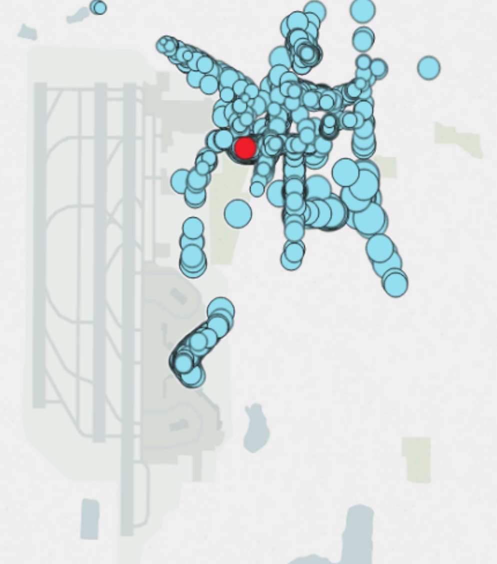
By building a model for each cell tower of how its signals should appear from different positions, we can flag cell tower transmissions that do not match those expected from a legitimate cell tower. This image shows all the measurements of cell ID 7843, where darker colors are stronger signal strengths and larger sizes represent how statistically unlikely the measurement is. Notice the very unlikely measurement towards the bottom.

Unusual Channels

To avoid interfering with the underlying network, IMSI-catchers may imitate nearby towers but broadcast on different frequencies (also known as channels). Most cell towers transmit on one or maybe two frequencies. If a cell tower appears to be transmitting on many frequencies over time then there may be a mimicking IMSI-catcher nearby.

This time series image shows an unusual set of measurements broadcasting on 6 different channels for the same cell ID. These were detected in front of a United States Citizenship and Immigration Services building (USCIS, a component of the DHS) south of Seattle. For comparison, no other tower in Seattle or Milwaukee was found to have transmitted on more than 3 channels, and over 96% of the cell towers were measured to have only transmitted on a single channel. Different colors in the image represent different channels, and sizes represent received signal strength. Notice the unusual cluster of channels detected near the USCIS building.





Unexpected Broadcast Properties

Every cell tower broadcasts configuration properties that are used to adjust cell phone transmissions and report the tower's supported features. These properties tend to be idiosyncratic, but are mostly the same between cell towers located in the same city, operated by the same cellular provider (like AT&T or T-Mobile). SeaGlass learns the distribution of these properties for each carrier as it collects the broadcasts from towers across a city.

IMSI-catchers must broadcast themselves as belonging to a particular network. Unless IMSI-catchers have been configured to perfectly mimic the particular properties used by the network it is imitating (which vary by network and city), they will be identifiable.

To see this in action, this image shows the measurements of the same cell ID near the Seattle-Tacoma International Airport. Broadcasts from this tower were measured over 2000 times over two months, and its broadcast properties were stable and in range of other towers from the same network. However, there was one highly unusual measurement where SeaGlass recorded broadcast properties for this tower that were well outside the range expected for any tower in the city. The red point is the anomalous measurement with four unusual BCCH properties (MSTXPWR, RXACCMIN, CRH, and T3212).

Changes over Time

Unlike normal cell towers, many IMSI-catchers are designed to be portable and transmit for short durations, just long enough to surveil a target of interest. There are some cases where legitimate cell towers will be moved to deal with a temporary increase in demand, like a sporting event, but this is relatively uncommon. Therefore, any shortly transmitting cell tower is suspicious and should be investigated. We found some temporary towers in the dataset, but further investigation suggests they resemble cell towers turned off for routine maintenance.

Validating the Results

We are currently working to corroborate our findings with secondary sources of information, like public records requests, to validate our results. SeaGlass was able to detect many suspicious anomalies, however, until they are independently verified, we can not definitively say the anomalies were caused by IMSI-catchers.

Technical Details

For more details on the SeaGlass sensors, data collection system, detection algorithms, and results see our technical paper published at Privacy Enhancing Technology Symposium 2017. Sensor code is available on Github.

Our Team

Peter Ney (left)
Computer Science and Engineering Ph.D. student at University of Washington

Ian Smith (right)
Research Scientist in Computer Science and Engineering at University of Washington

Tadayoshi Kohno

Professor of Computer Science and Engineering at University of Washington

Gabriel Cadamuro

Computer Science and Engineering Ph.D. student at University of Washington

We can be reached for questions and comments at
seaglass@cs.washington.edu
GPG fingerprint: 767A EAD9 0CA3 CD32 59E0 99F2 2CFB 213D D78C 351A

Subscribe to our SeaGlass mailing list for updates

email address

Subscribe

Acknowledgments

This project was supported by a grant from the John S. and James L. Knight Foundation and with help from the University of Washington's Tech Policy Lab.

KNIGHT FOUNDATION

TECH POLICY LAB

We also want to thank our volunteer drivers in Seattle and Milwaukee for their help collecting data for this project. Thank you!

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

seaglass@cs.washington.edu